New Rock Technologies, Inc.

SX3000 Enterprise Session Border Controller (SBC)

Administrator Manual

Website: http://www.newrocktech.com
Email: gs@newrocktech.com

Document version: 201504

Contents

Contents of Figure

Contents of Table

1 Device Structure

1.1 Front Panel

Figure 1-1 SX3000 front panel

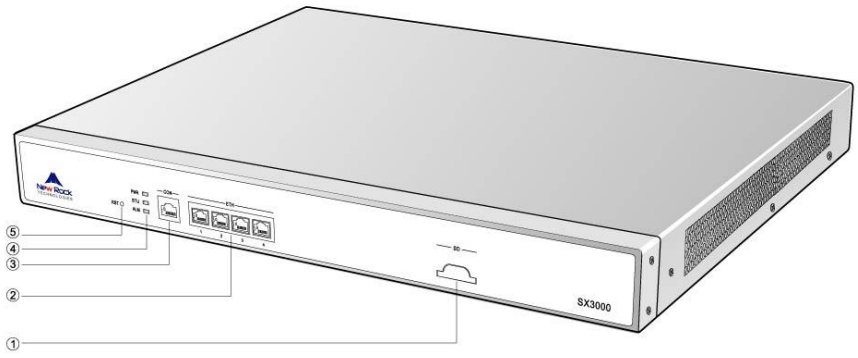


Table 1-1 Description of SX3000 front panel

#	Description
①	SD card port
②	4 ETH ports
③	CON port
④	Status indicators. For details, see Table 1-2.
⑤	Reset button. Press and hold down (with a thin object like a paper clip) for three seconds to restore factory settings.

Table 1-2 Indicators on the SX3000

LED	Color/status	Description
PWR	Green	Power on
	Off	Power off
STU	Off	System failed and inactive.
	Red for 10 seconds then turns solid green	When the indicator turns red, the system is powered up. When the indicator turns solid green, the system is operating normally.
	Green	The system is operating normally
ALM	Green	No alarms
	Red for 10 seconds then turns solid green	When the indicator turns red, the system is powered up. When the indicator turns solid green, the system is operating normally.
	Red	An alarm occurs.

1.2 Back Panel

Figure 1-2 SX3000 back panel

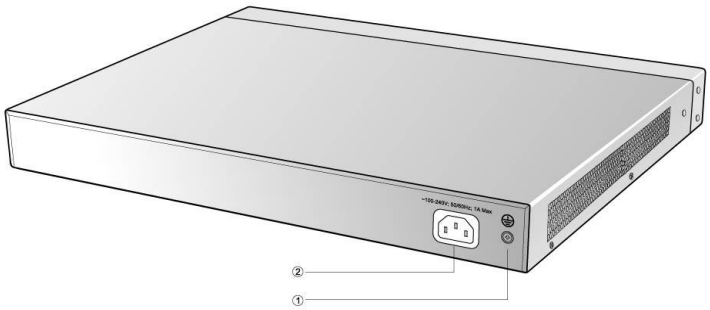


Table 1-3 Description of SX3000 back panel

#	Description
①	Ground pole
②	AC power socket, 100-240 VAC voltage input

1.3 Ethernet Port

There are four 10/100/1000M Ethernet ports on the SX3000 main control module, RJ45 with status LED. Table 1-4 shows the pin assignment of those Ethernet connectors and LED status specification.

Table 1-4 Ethernet port pin assignment

Rate	Pin							
	1	2	3	4	5	6	7	8
1000Base-T	BIDB-	BIDB+	BIDA-	BIDD-	BIDD+	BIDA+	BIDC-	BIDC+
100Base-TX/ 10Base-T	Tx+	Tx-	Rx+	Reserved	Reserved	Rx-	Reserved	Reserved

Table 1-5 Status LED specification

LED	Color/status	Description
Left side	Solid green	Port is connected successfully, but no traffic is available.
	Blinking green	Port is connected successfully, and traffic is available.
	Off	Port is not connected or fails to be connected.
Right side	On	Port operating at 1000 Mbps.
	Off	Port operating at 100 Mbps or 10 Mbps.

1.4 CON (Console) Port

SX3000 supports configuration through a console port (CON) of RJ45 connector. Table 1-6 shows the pin assignment and connector interface scheme of RJ45.

Table 1-6 Console port pin assignment of RJ45

RJ45 Connector Pin No.	1	2	3	4	5	6	7	8
Pin Description	NC	NC	TXD	GND	GND	RXD	NC	NC
DB9 Female Connector Pin No.			2		5	3		
DB25 Male Connector Pin No.			3		7	2		

The console port is used for local management and testing. PCs can be connected to SX3000 by linking the RS232 port to SX3000 console port. SX3000 uses three wires on the console port: one TXD (send), one RXD (receive), and one GND (ground). Table 1-7 shows the attribute of the console port.

Please use a RJ45 to RS232 serial cable as shown below for connecting the CON port on SX3000 side and the RS232 port on PC side. If the connection is established between SX3000 and the mobile PC with no RS232 ports, please use the cable together with USB to RS232 converter cable as shown below.

Figure 1-3 RJ45 to RS232 serial cable

Figure 1-4 USB to RS232 converter cable

Table 1-7 Console port specification

Attribute	Description
Connector Type	RJ45
Port Number	1
Port Type	RS232
Baud Rate	115,200
Data Bits	8
Parity Check	No
Stop Bit	1
Flow Control	No

2 Parameter Settings

2.1 Login

Note: You can log in to the device Web interface using browsers such as IE9-IE11, Firefox, and Chrome. The IE browser is used in the example below.

Enter the IP address of SX3000 in the address bar of the browser. Note that the default ETH1 address is 192.168.2.240. On the login interface, enter the username, password, and verification code to enter the configuration interface.

Note

If you access the device using HTTPS and have not installed the security certificate, the following error message will be displayed: *There is a problem with this website's security certificate.* In this case, click **Continue to this website**. If you use the default certificate and public/private key pair, the system will be at risk. You should replace them with the certificate and public/private key pair of your company.

Figure 2-1 Login interface

Login users are classified into **administrator** and **operator**. For the default password, see Table 2-1.

Note

To eliminate a security risk, please change the default password on the **System Tools** interface after

first login.

Table 2-1 Default Login Password

User	Default password	Description
admin	SX3000@123 (Upper case is required.)	An administrator can configure all parameters.
operator	operator@123 (Lower case is required.)	An operator can only view some parameters.

Note

- The SX3000 supports concurrent access from multiple users. When multiple users are accessing the SX3000, the administrator accessing the device first is allowed to modify configuration, and subsequent administrators are only allowed to view the configuration.
- The verification code for login is valid for 90 seconds. Upon expiration of the verification code, please click **Refresh** to generate a new verification code, and then enter it.
- When logging in using the **admin** account, if the password is entered incorrectly three times, the account will be inaccessible for 10 minutes, but the **operator** account is allowed. When logging in using the **operator** account, if the password is entered incorrectly three times, the IP address will be forbidden for 10 minutes.
- If the username is entered incorrectly six times, the IP address will be forbidden for 10 minutes.
- The system will confirm timeout if users do not conduct any operation within 10 minutes after login. They are required to login again for continuing operations.
- Upon completion of the configuration, click **Logout** to return to the login page, so as not to affect the login permission of other users.

2.2 Buttons Used on Management Interface

Submit Button: Submit configuration information. Users click **Submit** after completion of parameter configuration. A success prompt will appear if configuration information is accepted by the system; if a "The configuration takes effect after the system is restarted" dialog box appears, it means that the parameters are valid only after system restarts; it is recommended that users press the **Restart** on the *Tool* page to validate the configuration after changing all parameters to be modified.

2.3 Network Configuration

ETH1 is the factory default Ethernet port. If multiple Ethernet ports are used, it is necessary to ensure that their addresses are not on the same network segment.

After login, click **Network** to launch the configuration interface.

Figure 2-2 Network configuration interface

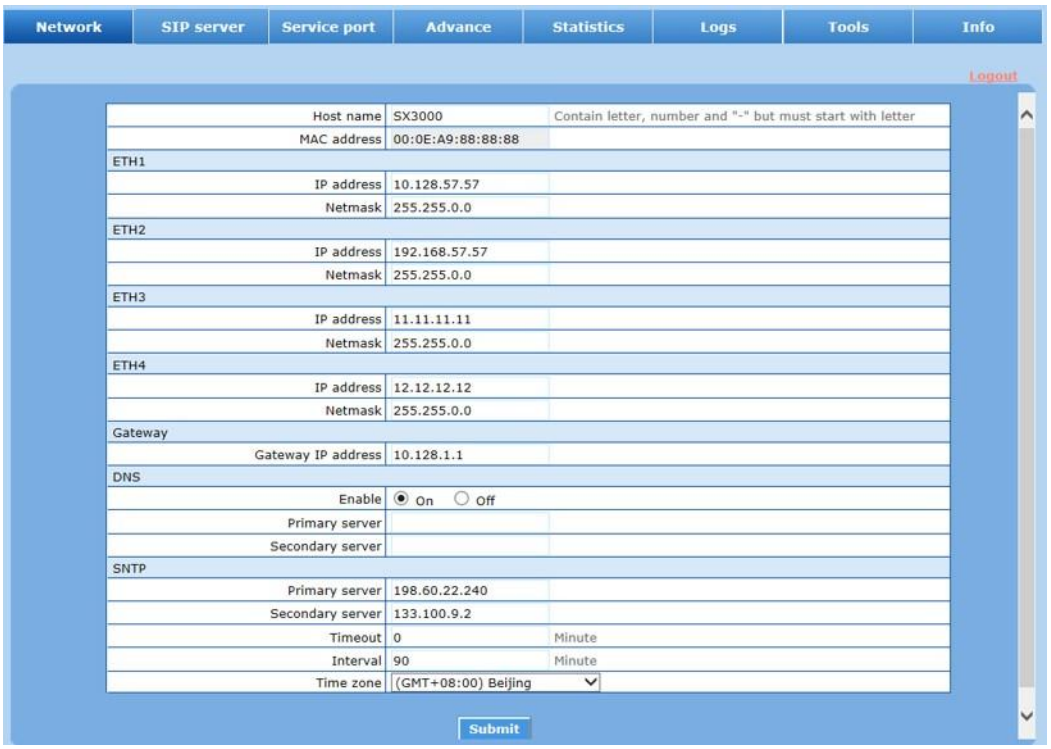


Table 2-2 Network configuration parameters

Name	Description
Hostname	The default value is SX3000. Users can set a different name for each device to distinguish from each other according to the deployment plan. The hostname may be a maximum of 48 characters. It can be upper-case letters A-Z, lower-case letters a-z, numbers 0-9, plus sign (+), or an IP address. The hostname cannot be null or empty. If the host name is not an IP address, its first character must be a letter, and its last character cannot be a minus sign.
MAC address	The MAC address of the device is displayed here.
ETH port n	
IP address	Enter the IP address of the ETH port n. Note: If only one ETH port is required, you can configure any one of the four ETH ports. If multiple ETH ports are required, their IP addresses must be on different network segments.
Netmask	Enter the netmask of the ETH port n.
Default gateway	
Gateway IP address	Enter the IP address of the default gateway.
DNS	
Enable	Activate DNS service.
Primary server	If DNS service is activated, the network IP address of preferred DNS server must be entered, and there is no default value.
Secondary server	If DNS service is activated, the network IP address of standby DNS server can be entered here. It is optional and there is no default value.
SNTP	
Primary server	Enter the IP address of preferred time server here. This parameter must be set due to no default value.
Secondary server	Enter the IP address of standby time server here. This parameter is optional. No default value is available.

Name	Description
Timeout	If the server is not located within the time allowed, SX3000 will try to locate it again. Unit: minute
Interval	Enter the time interval at which SX3000 will synchronize its time with the time server. Unit: minute
Time zone	Select a time zone, and the parameter values include: • (GMT-11:00) Midway Island • (GMT-10:00) Honolulu. Hawaii • (GMT-09:00) Anchorage, Alaska • (GMT-08:00) Tijuana • (GMT-06:00) Denver • (GMT-06:00) Mexico City • (GMT-05:00) Indianapolis • (GMT-04:00) Glace Bay • (GMT-04:00) South Georgia • (GMT-03:30) Newfoundland • (GMT-03:00) Buenos Aires • (GMT-02:00) Cape Verde • (GMT) London • (GMT+01:00) Amsterdam • (GMT+02:00) Cairo • (GMT+03:00) Moscow • (GMT+03:30) Teheran • (GMT+04:00) Muscat • (GMT+04:30) Kabul • (GMT+05:30) Calcutta • (GMT+05:00) Karachi • (GMT+06:00) Almaty • (GMT+07:00) Bangkok • (GMT+08:00) Beijing • (GMT+09:00) Tokyo • (GMT+10:00) Canberra • (GMT+10:00) Adelaide • (GMT+11:00) Magadan • (GMT+12:00) Auckland

2.4 SIP server Configuration

Depending on the SIP server deployment requirements, the SX3000 can send response messages to a designated port, or the sending port on the SIP server.

Click **SIP server** and enter the configuration interface.

Figure 2-3 SIP server configuration interface

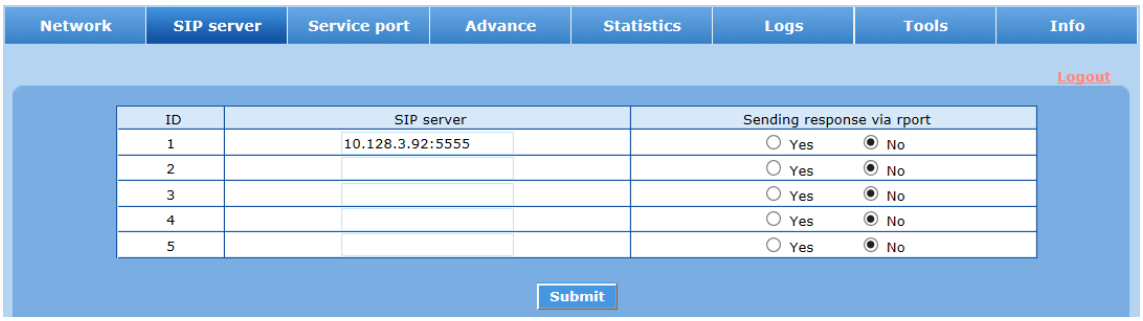


Table 2-3 SIP server configuration parameter

Name	Description
SIP server 1-5	IP addresses and port numbers of SIP servers are separated by ":". For example: 220.248.118.50:5060.

Note

- This parameter cannot be configured as localhost, 127.0.0.1, 0.0.0.0 or the IP address of SX3000.
- When forwarding a message to SIP server, SX3000 will select the port on the same network segment with the IP address of SIP server as the preferred one, while the port on the same network segment with the default gateway as the alternate one.

2.5 Service Port Configuration

The service port is used to receive the SIP messages from terminals, which will be processed and redirected to the SIP server associated to the port.

Up to 5 service ports can be configured on SX3000, each associated with a primary SIP server and its backup SIP servers.

The SX3000 may choose to encrypt and decrypt the messages sent and received by each service port. It may encrypt and decrypt voice and signaling separately or simultaneously. By default, the SX3000 does not encrypt or decrypt messages. When the encryption is selected, SX3000 will perform decryption to the received messages from terminals before they are redirected to the SIP server; similarly, SX3000 will perform encryption to the messages from the SIP server before they are sent to the terminals.

Encryption key may be needed for some encryption methods (except for UDP Encrypted and TLS), and the key used should be identical on both SX3000 and the terminals.

When TLS encryption method is selected, SRTP will be used to encrypt RTP packets.

Four Eth ports of SX3000: Eth 1, Eth 2, Eth 3 and Eth 4. Different parameters should be applied according to different Eth ports. Users can configure corresponding configuration of each Eth port. Take "Eth 1" for example.

After login, click **Service port** > **Eth 1** to launch the configuration interface.

Figure 2-4 Service port configuration interface

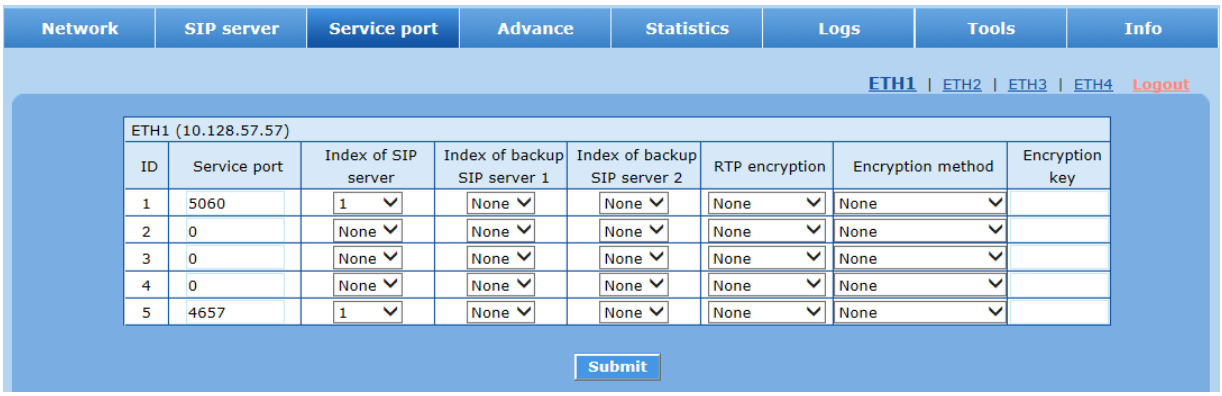


Table 2-4 Service port configuration parameter

Name	Description
Eth 1 (IP address)	Display IP address of Eth 1 which is configured at **network** parameter configuration. (Read only)
Service port	Configure the service port for receiving signaling messages from terminals.
Index of SIP server	Configure the SIP server corresponding to the service port. SIP server No. 1–5 are supported right now.
Index of backup SIP server	Each service port can be configured with two backup SIP servers: backup SIP server 1 and backup SIP server 2. After the heartbeat monitoring function is enabled on the SX3000, if a SIP server goes down, the SX3000 will automatically switch to a backup SIP server. After the original SIP server returns to normal, the SX3000 will automatically switch back to it.
RTP encryption	Three encryption schemes: • None: non-encryption; • RTP: perform encryption on all of the RTP packet; • RTP Header: perform encryption only to the headers of RTP packets; • RTP Body: perform encryption only to the bodies of RTP packets.
Encryption method	Eight encryption schemes: • None: non-encryption • TLS • TCP Not Encrypted: package signaling (RTP) by TCP; non-encryption • TCP Encrypted: package signaling (RTP) by TCP Protocol; encryption used • UDP Not Encrypted: package signaling (RTP) by UDP; non-encryption • UDP Encrypted: package signaling (RTP) by UDP; encryption used • Using Keyword • Using Keyword2 • Encrypt 14
Encryption key	Set the encryption key here. If a terminal requires encryption, its encryption key must be the same as that of the SX3000. For UDP Encrypted and TLS, no encryption key is required.

2.6 Advanced Configuration

2.6.1 System

After login, click **Advance > System**.

Figure 2-5 Interface for advanced system configuration

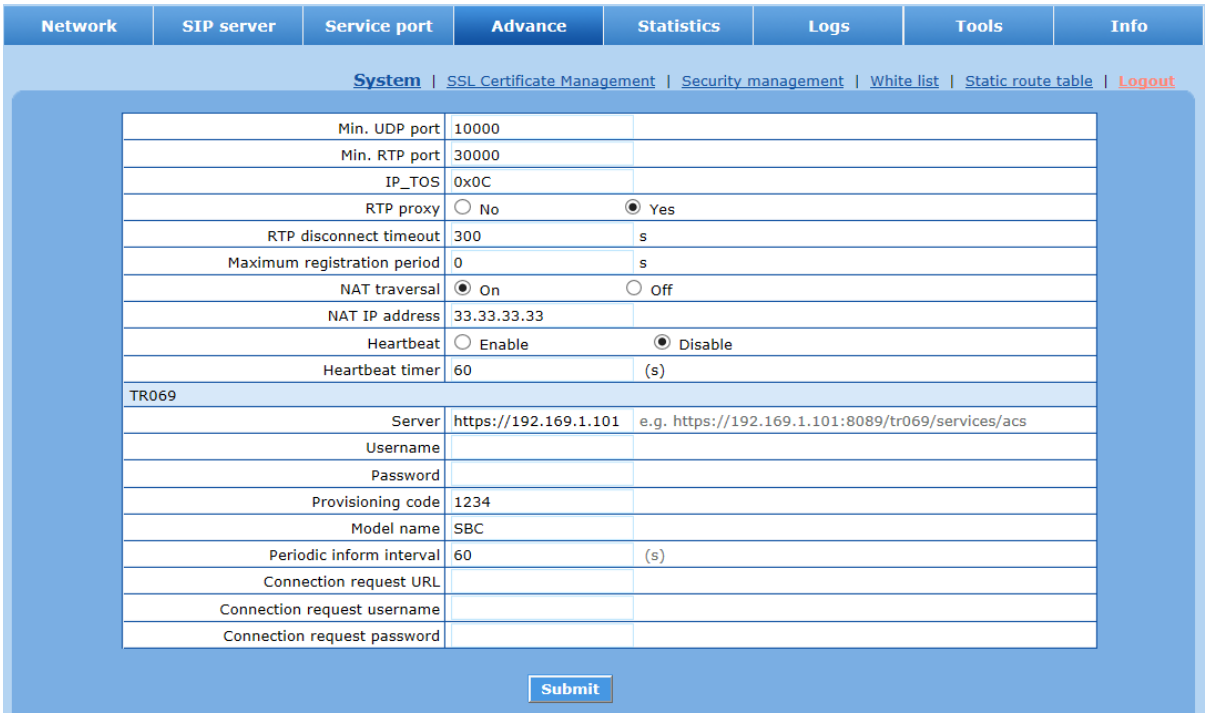


Table 2-5 Parameters of system advanced configuration

Name	Description
Min. UDP port	This port is used to exchange packets with the SIP server. The port number must be smaller than the min. RTP port number. By default, the port number is 10000. The UDP port number ranges between the min. UDP port number and (the min. RTP port number –1).
Min. RTP port	Min. port number that is used to send and receive RTP voice packets. It must be larger than the min. UDP port number. It is 30000 by default. The RTP port number ranges between the min. RTP port number and the min. RTP port number + 4799.
IP_TOS	To define QoS of different levels. Default value: 0x00. Example: TOS=0xB8 indicates that the previous level is 5. Low time delay & high throughput is required. No requirements for the stability.
RTP proxy	To configure whether RTP is transmitted by SX3000.
RTP disconnect timeout	Close RTP Port if there's no RTP message transmission during configuration time interval. Valid range: 180-1,200 seconds. It is 300 seconds by default.

Name	Description
Maximum registration period	The maximum period allowed for forwarding the registration messages sent from terminal to SIP server via SBC. It is 0 by default. • If the default period is used, SBC will not check the exprise value carried by terminal registration message, therefore the terminal registers with its original period; • If entering the maximum registration period more than exprise value, the terminal registers with the maximum registration period entered. • If entering the maximum registration period less than exprise value, the terminal registers with its original period.
NAT traversal	• On: the IP addresses carried by Via and Contact field of terminal message is revised into the ones of SX3000. • Off: non-revise.
NAT IP address	To ensure communication between the SX3000 deployed behind a NAT device and the terminals on public network, you should enter the public IP address of the NAT device here, then perform the following port mapping on NAT device: • Map the address of the ports connecting to the terminals on public network to the public IP address of NAT device. • Perform port mapping on the service ports connecting to the terminals on public network. For example, if ETH1 is selected to connect the NAT device, the one-to-one port mapping is performed on all the service ports displayed on the **Service Port>ETH 1** interface. • Perform port mapping on the UDP ports and RTP ports activated on SX3000 ranging from the min. UDP port number to the min. RTP port number added by 4,799. For example, assuming that the min. UDP port number and RTP port number obtained from **Advance>System** interface are 10,000 and 30,000 respectively, the port mapping is required to perform on the ports ranging from 10,000 to 34,799.
Heartbeat	The heartbeat for detecting the status of SoftCo.
Heartbeat timer	Intervals at which OPTIONS messages are sent to the SIP server.
TR069	
Server	Enter the IP address of the TR069 network management system. HTTP and HTTPS are supported.
Username	Enter the username of the administrator.
Password	Enter the password of the administrator.
Provisioning code	Only digits and characters are permitted.Identifier of the device provider.
Model name	A character string that describes the interface type or name.
Periodic inform interval	In second.Intervals at which a report (measured in seconds) is sent to the TR069 network management server.
Connection request URL	HTTP URL for an ACS to make a Connection Request notification to SX3000.
Connection request username	Username used to authenticate an ACS making a Connection Request to the SX3000.
Connection request password	Password used to authenticate an ACS making a Connection Request to SX3000.

2.6.2 SSL Certificate Management

After login, click **Advance** > **SSL Certificate Management**.

Figure 2-6 SSL certificate management interface

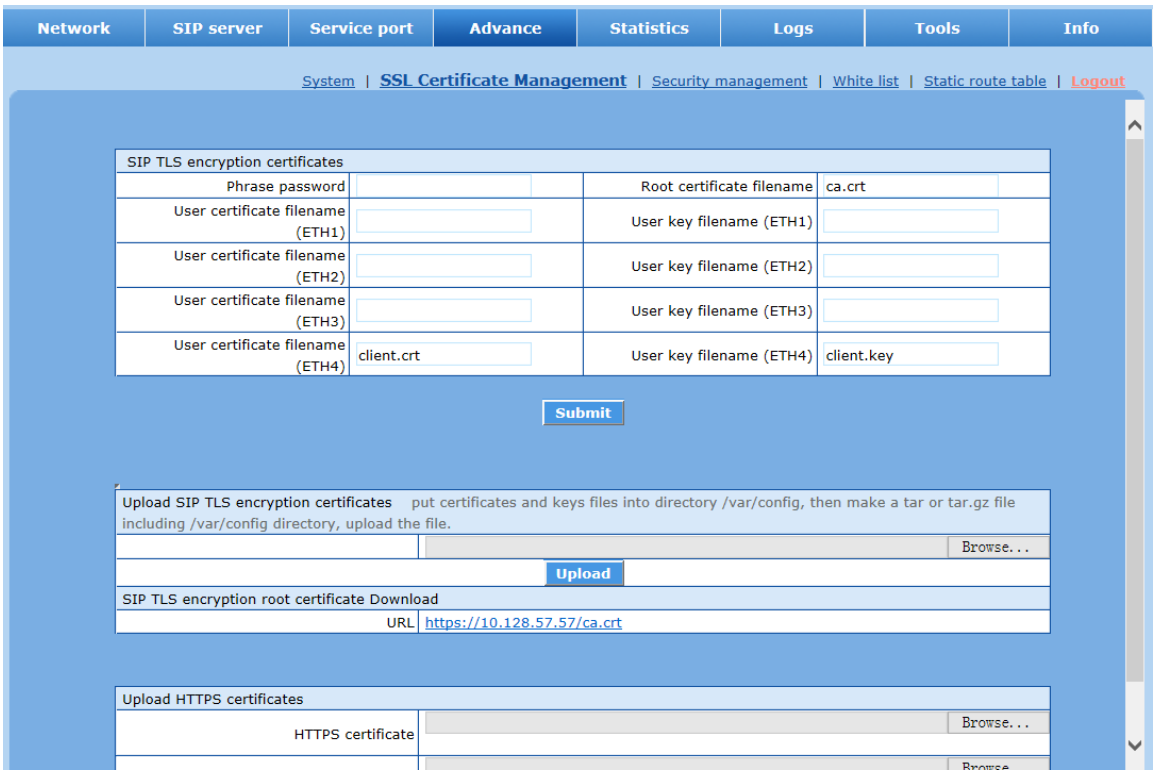


Table 2-6 SSL certificate management configuration parameters

Name	Description
Phrase password	Password that needs to be entered when creating the SIP TLS encryption certificate. See the section “Creating an SIP TLS Encryption Certificate” in the *Configuration Guide*.
Root CA certificate filename	Name of the created SIP TLS root certificate file. See section “Creating an SIP TLS Encryption Certificate” in the *Configuration Guide*.
User certificate filename (ETH1/2/3/4)	The name of the file which contains the user certificate for ETH1/2/3/4. For information on how to create the user certificate, see section “Creating an SIP TLS Encryption Certificate” in the *Configuration Guide*.
User key filename (ETH1/2/3/4)	The name of the file which contains the user private key for ETH1/2/3/4. For information on how to create the user key, see section “Creating an SIP TLS Encryption Certificate” in the *Configuration Guide*.
Upload SIP TLS encryption certificates	Upload the created encryption certificate in .tar format. For details, see Step 5 in the section “Configuration Procedures” in the *Configuration Guide*.
URL for SIP TLS encryption root certificates	A URL is displayed here after a certificate is uploaded using SFTP. You can click on the link to download the SIP TLS encryption root certificate.
Upload HTTPS certificate	Upload the HTTPs certificate and key provided by the certificate authority. If you use the default certificate and public/private key pair, the system will be at risk. You should replace them with the certificate and public/private key pair of your company, and then import the root certificate using the browser on your PC.

2.6.3 Security Management

Telnet/SSH service can be enabled or disabled on the **Advance > Security** interface.

Flexible access control can be set for the SX3000. For details, see the Linux iptables operation manual.

Note

- By default, both the Telnet/SSH service and the ping operation are disabled on the device.
- After enabling the Telnet/SSH service on the device, disable it immediately after use. Otherwise your system will be at risk.
- When adding an access control command, add the path **/var/run/** before the command. For example:

  /var/run/iptables -A INPUT -s 10.128.23.23 -p tcp --dport 80 -j ACCEPT

  You can add or edit commands using a text box (one line for one command).
- If the access control configuration is incorrect, the device cannot be accessed through an ETH port.

After login, click **Advance** > **Security management**.

Figure 2-7 Security management configuration interface

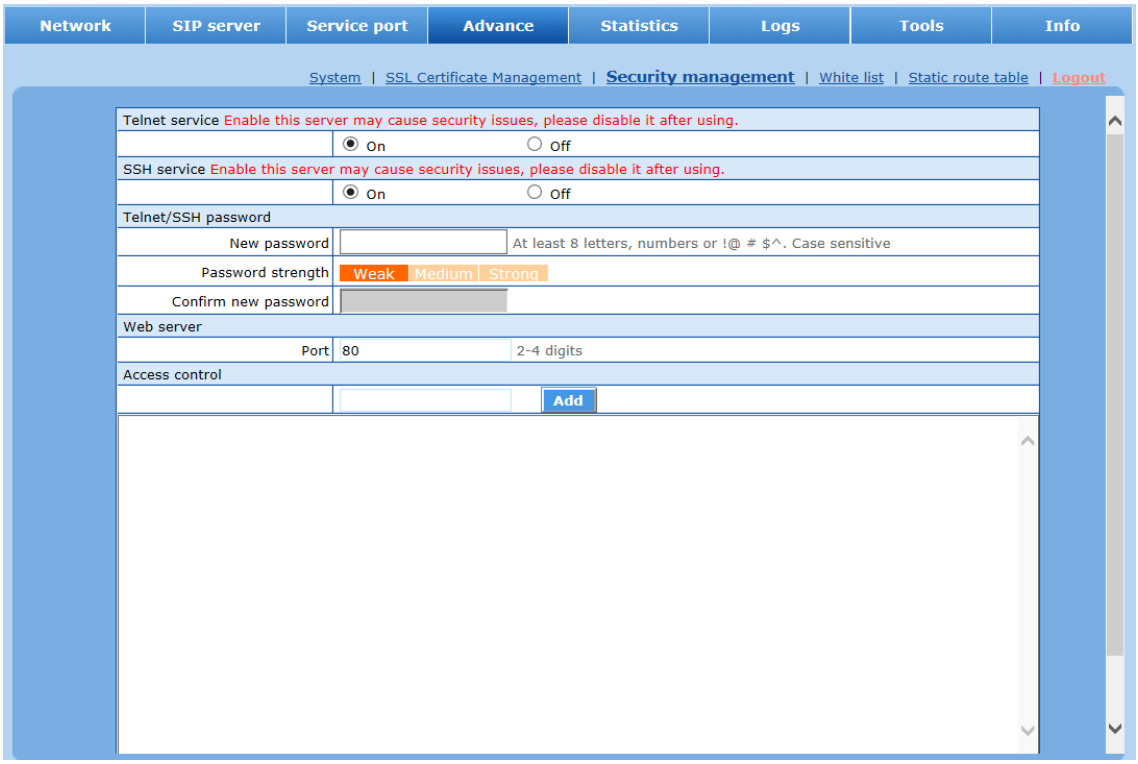


Table 2-7 Security management configuration parameters

Name	Description
Telnet service	By default, the HTTP and HTTPS ports are enabled on the SX3000. You can only access, manage, and maintain the device using a Web browser. By default, the Telnet and SSH services disabled. You can enable them if necessary. IP addresses of the access devices can be set on the whitelist interface.
Web server	The port used to access the device using a Web browser. By default, it is 80.

Name	Description
Access control	Example: • /var/run/iptables -A OUTPUT -d 192.168.250.230 -p icmp -j DROP This message will not ping to the host computer of the IP address which is 192.168.250.230. But it has no influence on other host computers. User may change the specified IP address to prevent Pinging corresponding host computers. • /var/bin/iptables -A INPUT -p tcp --dport 80 -s 192.168.250.230 -j DROP This message will not allow user to access host computer of IP address which is 192.168.250.230 to SX3000 by http, but it will not have influence on other host computers. User may change the specified IP address to prevent corresponding host computers accessing SX3000. • /var/run/iptables -F All rules that existed are eliminated

2.6.4 Whitelist

After the whitelist function is enabled, only the IP addresses on the whitelist are allowed to access the device using Web or Telnet.

Click **Advance** > **White list** to enter the interface.

Figure 2-8 Whitelist configuration interface

To configure the whitelist:

Step1 Click **Add**.

Step2 In the input box that is displayed, enter the allowed IP addresses, and then click **OK**.

Step3 Click **"On"** to enable the whitelist.

Note

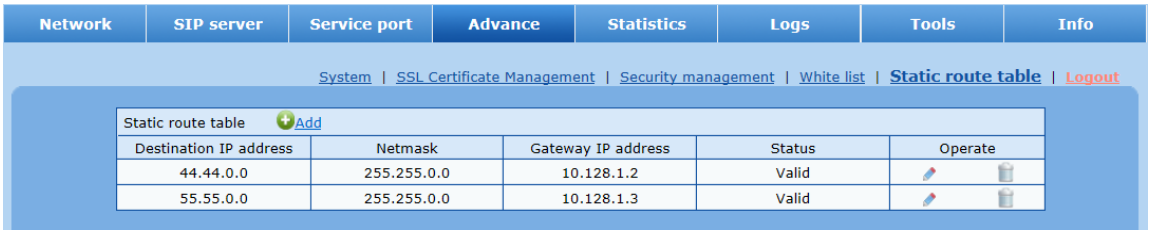
- No IP address segment can be configured.
- The device must be restarted to validate the configuration.
- To use the Telnet whitelist, you need to enable the Telnet service as shown in Figure 2-7.
- If the whitelist is enabled but empty, the device can be accessed from any IP addresses.
- A maximum of 30 IP addresses can be added on the whitelist.

2.6.5 Static Route Table

You can configure a static route table so the SX3000 can forward messages based on the set rules.

Click **Advance** > **Static** route table to enter the interface.

Figure 2-9 Static route table configuration interface



To configure a static route table:

Step1 Click **Add**.

Step2 In the input box that is displayed, enter the destination IP address, netmask, and gateway address. Click the Enable icon, and then click **OK**.

Note

- The route table configuration rules must be followed when configuring the IP address and netmask. The gateway address is the next-hop address.
- The device must be restarted to validate the configuration.

2.7 Call Status and Statistics

2.7.1 Online Devices

After login, click **Statistics** > **Online Devices** to launch the configuration interface. All Web login user information (IP address & level) and information of online gateways can be seen.

Figure 2-10 Online devices configuration interface

Table 2-8 Parameters of system status

Title	Explanation
Login User Info	The user IP address and identity of the login users are displayed here. The number following the IP address indicates the user identity: 1: The first administrator that accesses the device who is allowed to modify the configuration 2. The operator is only allowed to view the configuration. 3. The administrator that accesses the device after the first one is only allowed to view the configuration.
Online Gateways Info	Information about online terminals is displayed here. • total: Number of the online terminals • id: Serial Number of an online terminal • gw ip: rport: IP address and port number of an online terminal. • sbc ip:port: IP address and port number of the SX3000 • sbc udp local port: The local UDP port created by the SX3000 for the terminal. • ss sip:port: IP address and port number of the SIP server • protocol: Protocol used

2.7.2 Call Log

After login, click **Statistics** > **Call Log**.

Figure 2-11 Call log interface

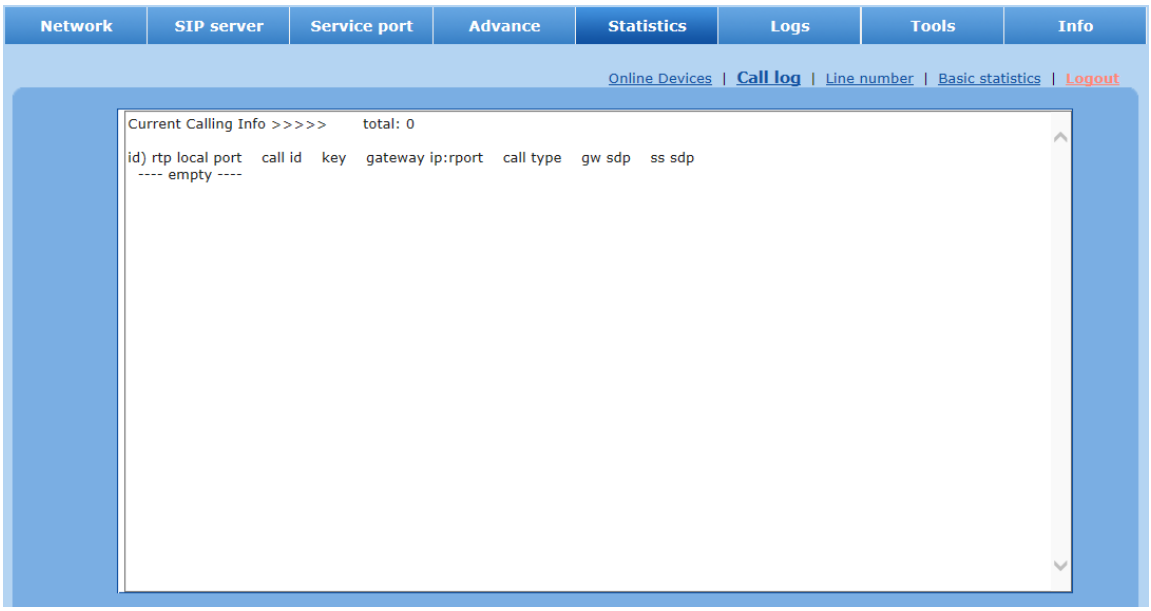


Table 2-9 Call log configuration parameters

Name	Description
Current RTP Call log Info	• total: The number of established calls • rtp local port: Local RTP port • gateway ip:rport: IP address and port number of an online terminal • call type: There are two types of call, incoming for inbound calls and outgoing for outbound calls • gw sdp: The SDP addresses of online terminals • ss sdp: The SDP address of SIP server

Note

If **RTP proxy** is set to **No** on the **Advance** > **System** interface, the RTP will not pass through the SX3000, and the **Call log** interface will be empty. In this case, you cannot view information about the voice stream.

2.7.3 Line Number

After login, click **Statistics** > **Line number** to launch the configuration interface.

Figure 2-12 Line number configuration interface

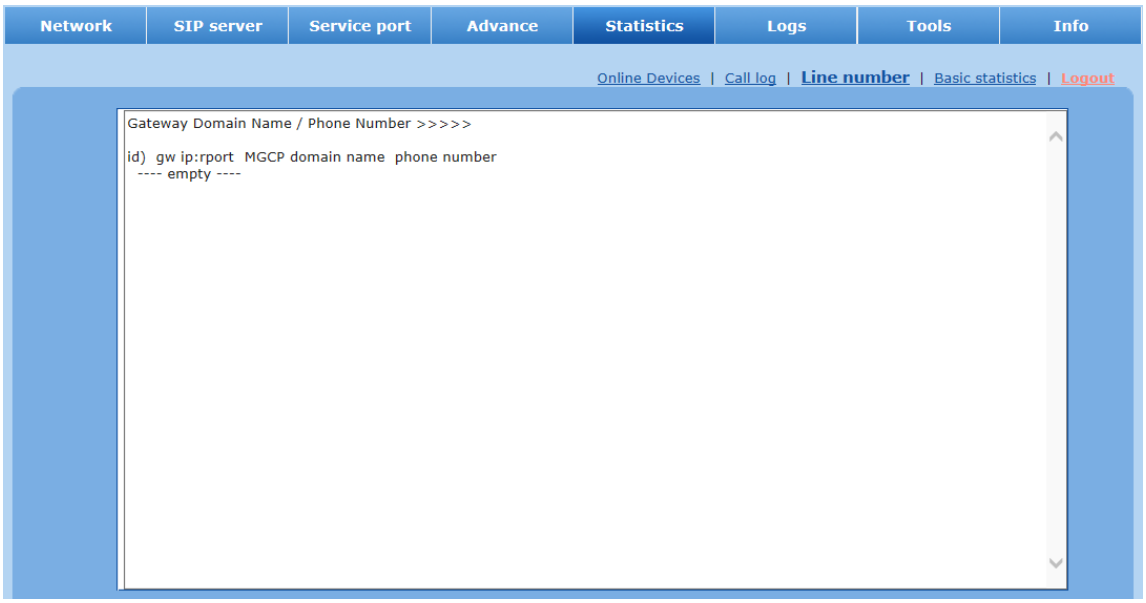


Table 2-10 Line number configuration parameters

Name	Description
Line number	• Id: ID of an online terminal • gw ip:rport: Address and port number of an online terminal • phone number: Phone number associated with the terminal

2.7.4 Basic Statistics

After login, click **Statistics** > **Basic statistics** to launch the configuration interface.

Figure 2-13 Basic statistics interface

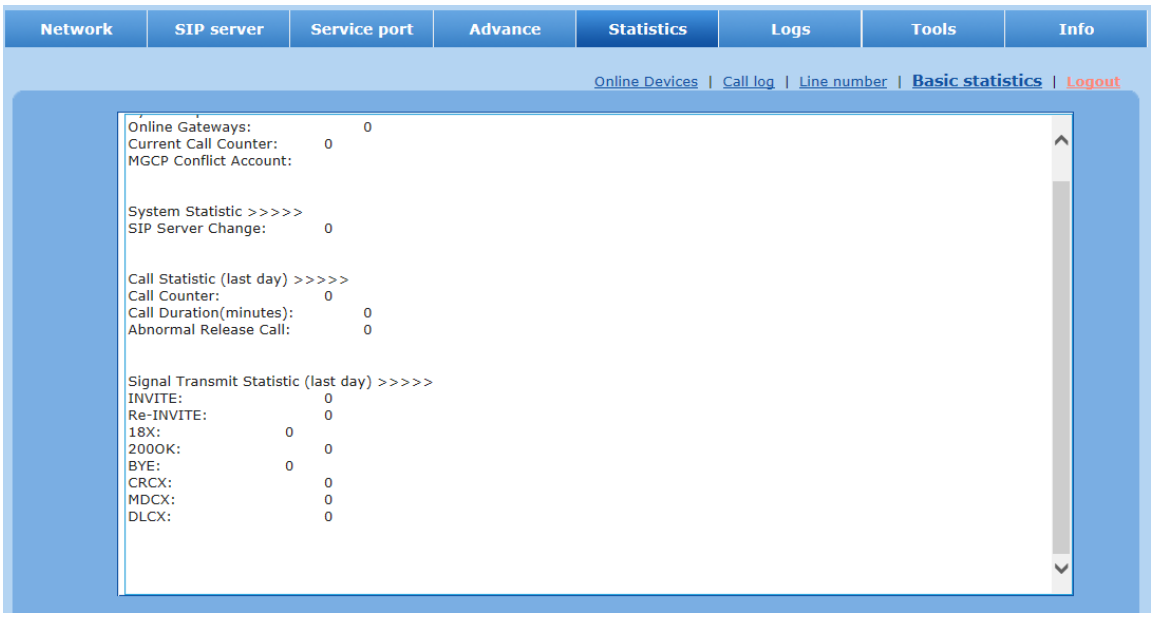


Table 2-11 Parameters of basic statistics

Parameter	Description
System Info	• System Up Time: System startup time • Online Gateways: Number of online terminals • Current Calling Counter: Number of undergoing calls
System Statistic	• SIP Server Change: Number of SIP server changes
Call Statistic	The following details about the calls placed within the last 24 hours are displayed here. • Call Counter: Number of calls placed within the last 24 hours. • Call Duration (minutes): Duration of all calls placed within the last 24 hours, measured in minutes. • Abnormal Release Call: Number of the calls that are connected within the last 24 hours but no BYE signaling is received.
Signal Transmit Statistic	Number of the signaling messages (INVITE, Re-INVITE, 18X, 200OK, BYE, CRCX, MDCX, and DLCX) transferred within the last 24 hours

2.8 Log Management

2.8.1 Managing Log

After login, click **Logs** > **Managing Log**. Log files can be downloaded through this interface.
If no SD card is available on the device, the debugging log entries will be stored in RAM. If an SD card is available on the device, the debugging log entries will be stored in the SD card.

Note

Never insert or remove the SD card when the device is running as the device may run abnormally.

Figure 2-14 Interface of managing log-(without an SD card)

Table 2-12 Parameters of managing log-(without an SD card)

Name	Description
System log server	Set the IP address of system log server.
Debug log server	Set the IP address of debug log server.
Debug log level	Select a log level. A higher log level indicates more detailed log entries. By default, the log level is 3. Note: In normal operation the log level must not exceed 3, otherwise the device performance may be affected.

Figure 2-15 Debugging log management interface (with an SD card)

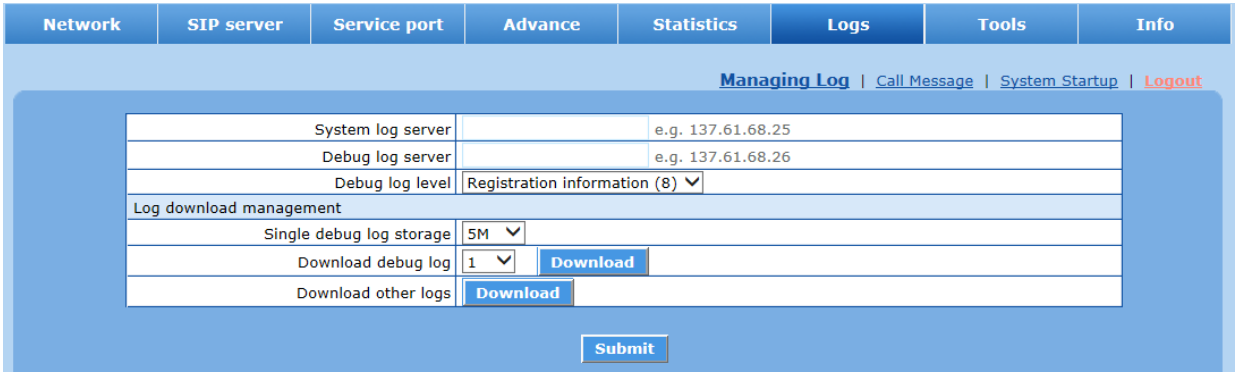


Table 2-13 Debugging log management interface (with an SD card)

Parameter	Description
System log server	Set the IP address of system log server.
Debug log server	Set the IP address of debug log server.
Debug log level	Select a log level. A higher log level indicates more detailed log entries. By default, the log level is 3. Note: In normal operation the log level must not exceed 3, otherwise the device performance may be affected.
Single debug log storage	Set the size of each debug log. An SD card can store at most 20 debugging log entries. If there are more than 20 log entries, the oldest ones will be overwritten.
Download debug log	Select the serial number of the debug log stored in the SD card, and then click **Download**. A larger serial number indicates a newer log. For the download procedure, see the description below.
Download other logs	Download other logs, including Web operation log, SSH background operation log, and debugging logs that are not stored in the SD card temporarily. For the download procedure, see the description below.

Procedure of downloading the debugging log:

Step1 Click **Download**.
The device starts packing the log.

Step2 Wait (time depends on the log size) until the log saving interface is displayed.

Step3 Click **Save as**, and select the path to save.

Step4 The user may review the log from the server concerned.

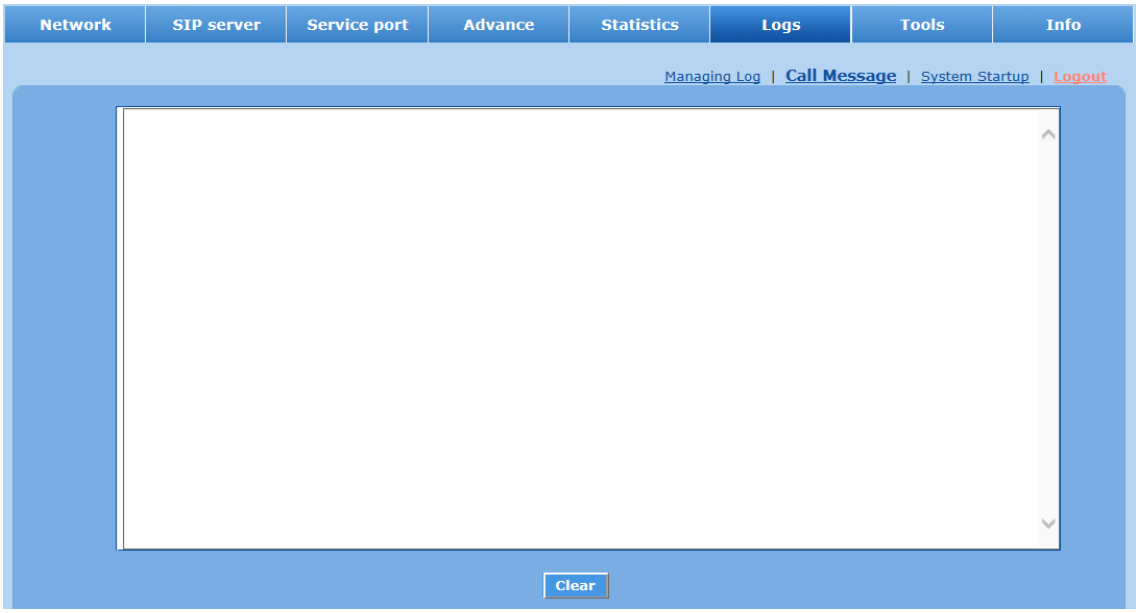
Note

If only 500 MB is available on the SD card, the system will automatically clear the outdated log files (namely, the log files generated five years ago).

2.8.2 Call Message

After login, click **Logs** > **Call Message**.

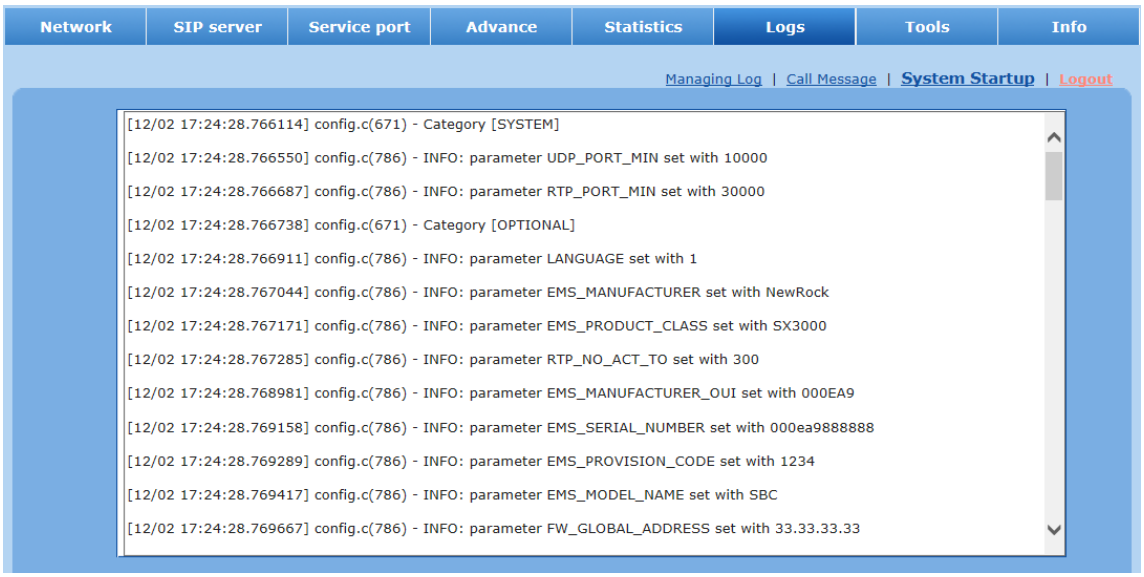
Figure 2-16 Call message interface



2.8.3 System Startup

After login, click **Logs** > **System startup**.

Figure 2-17 System startup interface



2.9 Tools

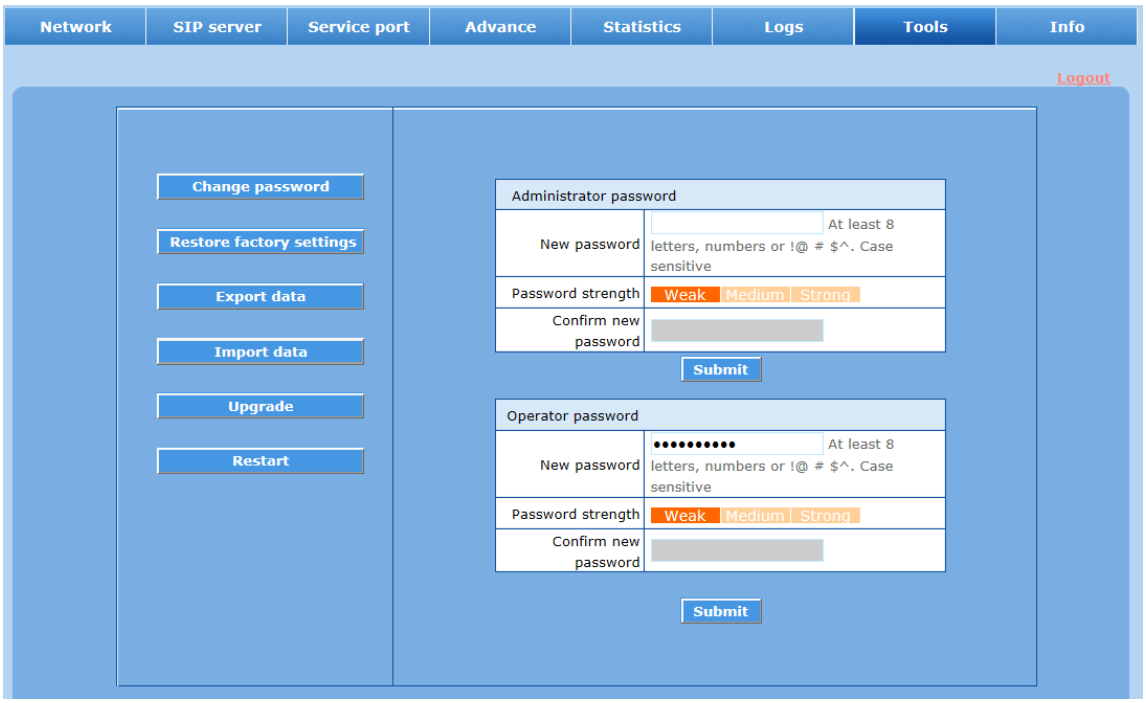
2.9.1 Change Password

After login, click **Tools** to open this interface. Only administrator is entitled to change the password of login.

For changing administrator password, it's required to enter new password into **New password** field and **Confirm new password** field, then click **Submit**.

The password being used by the operator will be displayed as hidden codes, which could be changed by the administrator at any time. The administrator is allowed to change the operator's password by entering the new password into **Operator password > password**.

Figure 2-18 Password changing interface



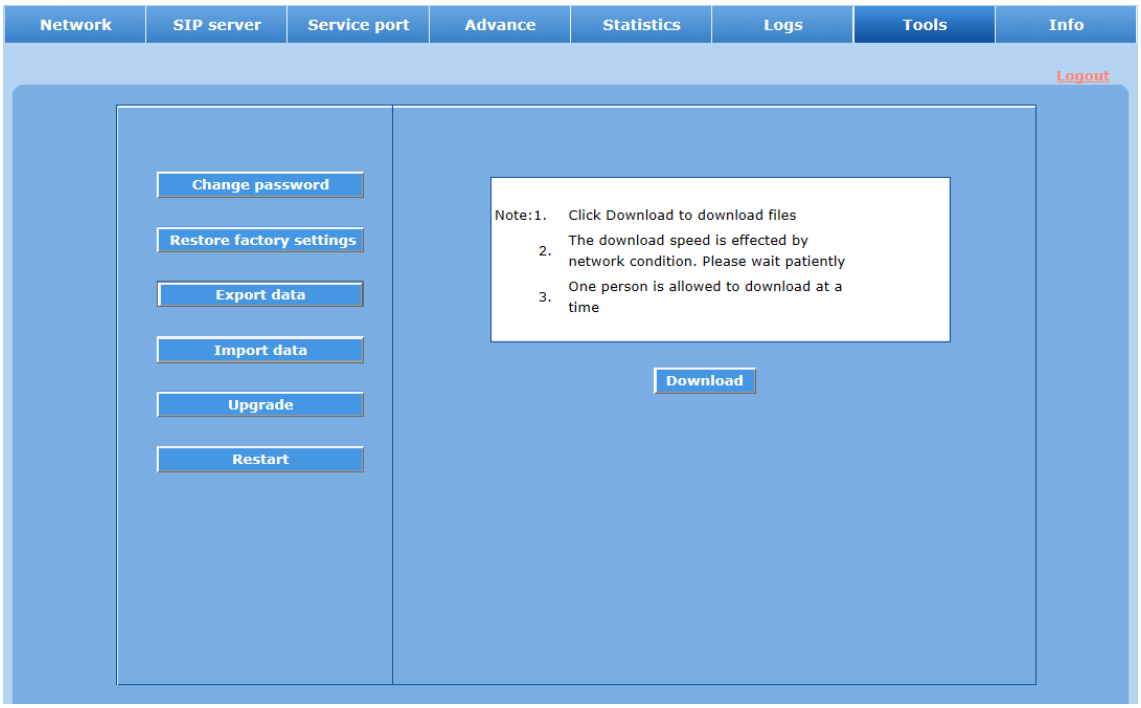
Note

The new password is displayed as implicit code.

2.9.2 Download Data

After login, click **Tools** > **Export data** to open this interface. The download procedure is similar to the one of log files.

Figure 2-19 Data downloading interface



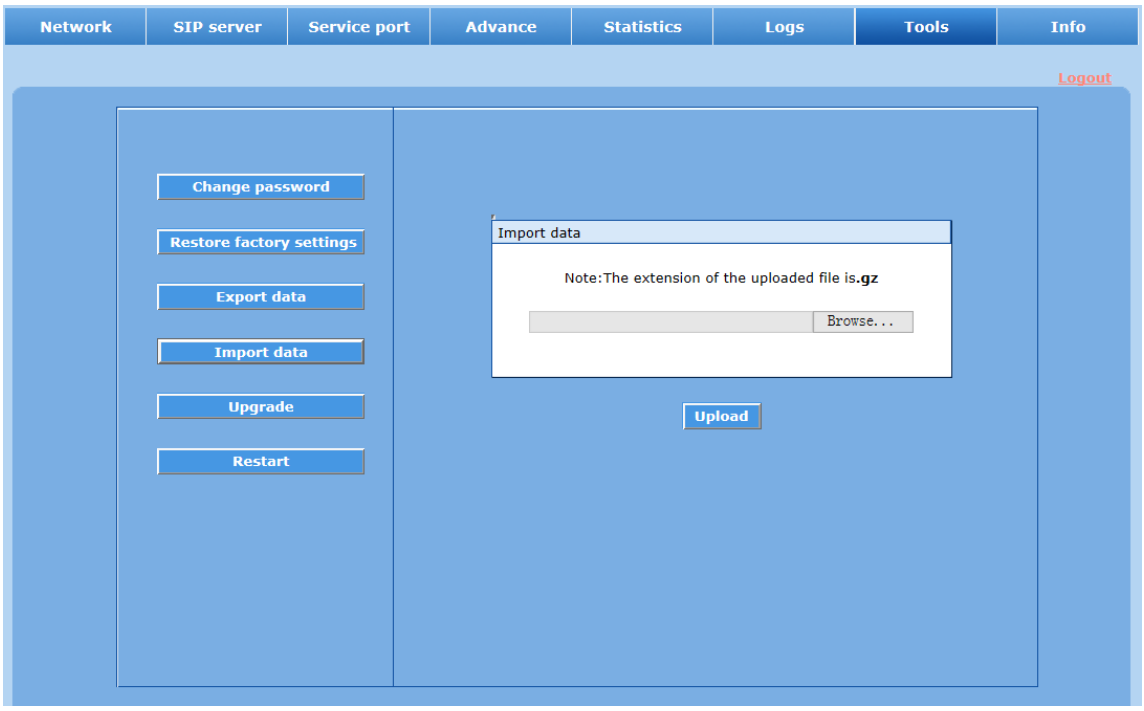
Note

The configuration of whitelist, security management (except the access control configuration), static route table, and network page cannot be downloaded.

2.9.3 Import Data

After login, click **Tools>Import data** to open this interface. Operating procedure is the same as that of software upgrade.

Figure 2-20 Data importing interface



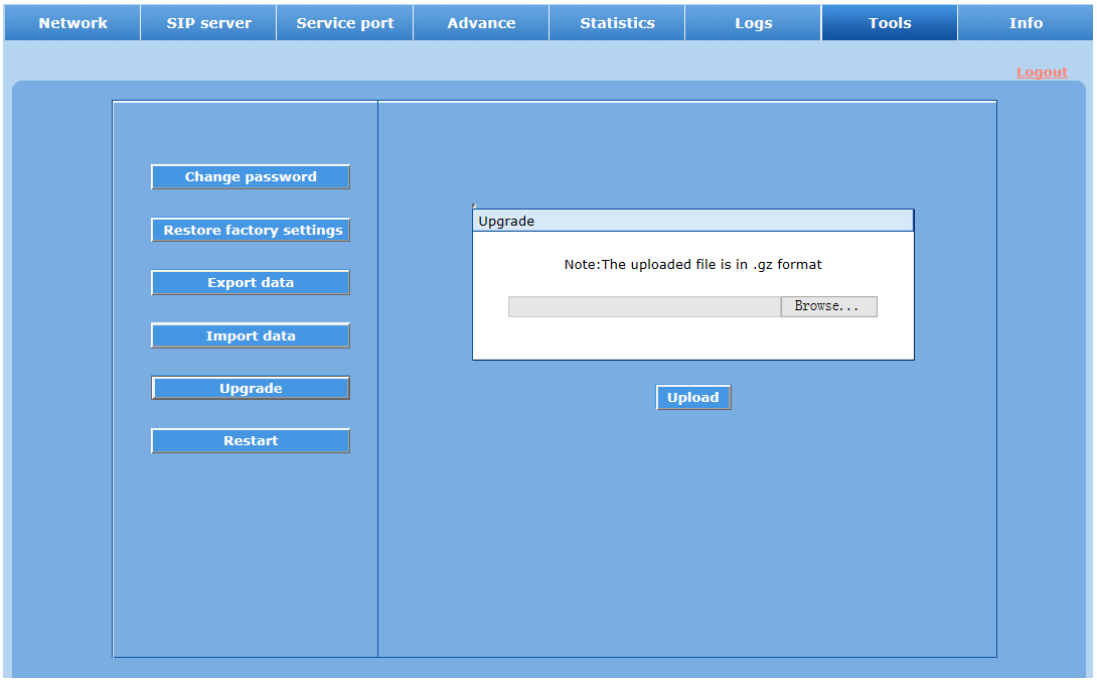
2.9.4 Upgrade

After login, click **Tools > Upgrade** to open this interface. The software upgrade procedure is presented as below:

Step1 Obtain the upgrade files (tar.gz file), and save the file onto a local computer.

Step2 Click **Tools > Upgrade** to access to the page of software upgrade.

Figure 2-21 Software upgrading for interface 1

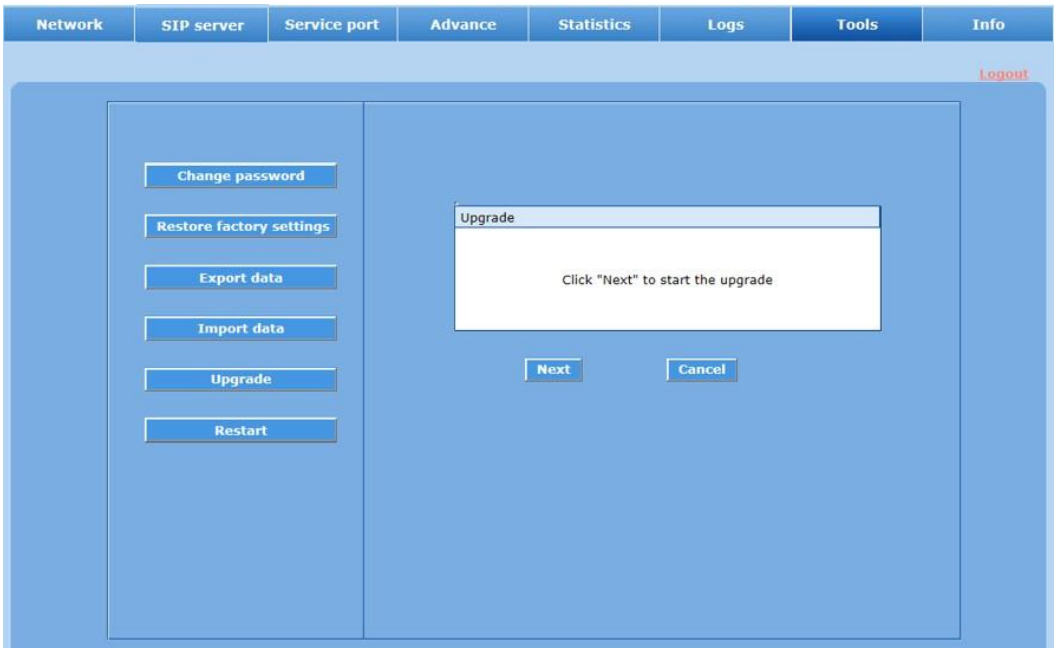


Step3 Click **Browse** to select the upgrade files.

Step4 Click **Upload**.

Step5 When the upload is complete, click **Next** to start the upgrade.

Figure 2-22 Software upgrading interface 2



Step6 When the system prompts that the software has upgraded successfully, it will ask you to restart the device. Click **OK**.

Note

- A few minutes are needed to upgrade the device. Do not shut down, disconnect, or restart the device during this period.
- The device is in the process of rebooting when the interface cannot be displayed.
- Wait for about two minutes, and access the interface of device management system, click **Version info** and check the software version.

2.9.5 System Reboot

After login, click **Tools** > **Reboot** to restart the device. As this is a system wide reset, it takes longer time.

2.9.6 Restore Factory Settings

After login, click **Tools** > **Restore factory settings** to restore the factory settings.

The factory settings are designed based on common applications, and therefore, no need to modify them in many deployment situations.

2.10 Version Information

After login, click **Version info** to view the device hardware and software version information.

2.11 Logout

After login, click the **Logout** at top right to exit the device management system and return to the login interface.